ATTORNEY GENERAL ROY COOPER
NORTH CAROLINA DEPARTMENT OF JUSTICE
A RESOURCE GUIDE FOR PARENTS

UPDATED
SEE PAGE 44

INTERNET SAFETY

what you don't know can hurt your child

The information in this Resource Guide represents current best practices as described by experts in the fields of Internet safety and law enforcement. Visit www.ncdoj.com to keep up with advances in the ongoing effort to keep our children safe on the Internet. You can also learn about scams, identity theft, viruses and other security-related issues involving the use of computers.

Many individuals helped make this Internet safety project possible. We would like to particularly thank Gail Barnes, John Bason, Jay Chaudhuri, Caroline Farmer, William McKinney, Noelle Talley, Julia White, and Carol Young of the North Carolina Department of Justice; Special Agent Kevin West and retired Special Agent Melinda Collins of the North Carolina State Bureau of Investigation and the North Carolina Internet Crimes Against Children Task Force; Nancy McBride of the National Center for Missing & Exploited Children; and Professor Tony Brock of the Department of Graphic Design at North Carolina State University.

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®
www.missingkids.com

This project was supported by federal funds formula grant projects # 2003-IJ-CX-K019 and 2003-GP-CX-0184, awarded by the Office of Justice Programs, United States Department of Justice. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the United States Department of Justice.

A total of 5,000 copies of this public document were printed by the North Carolina Department of Justice at a cost of $4,887 or $.98 per copy. These figures include only the direct costs of reproduction. They do not include preparation, handling, or distribution costs.

Computers and the Internet have revolutionized the way we communicate, work, shop and learn. But along with the positive changes come new responsibilities and potential dangers. Hazards that begin with innocent computer use can threaten your family's safety and well-being.

For example, child predators who cruise the playgrounds for victims now spend time cruising the Internet. In fact, a survey by the National Center for Missing & Exploited Children found that one out of every five young Internet users said that they had received an unwanted sexual solicitation online in the past year.

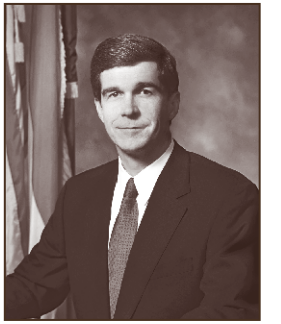
As a father of three daughters myself, I know that the challenge to parents is protecting children who are smart enough to use a computer, but not wise enough to protect themselves from online strangers or graphic websites.

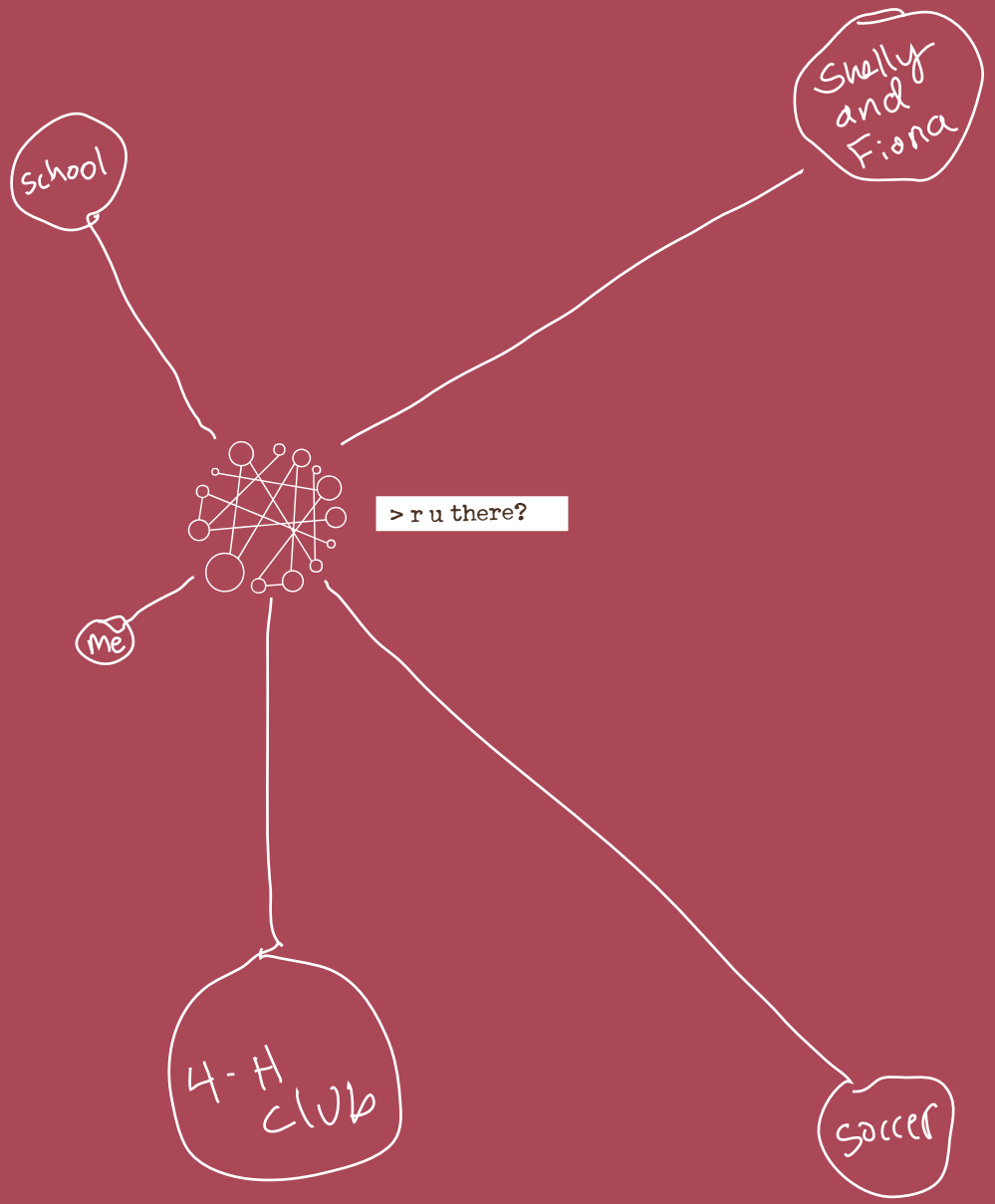
Just as you supervise how and when your children drive a car, you can monitor their use of the Internet. This guide and accompanying video are designed to help parents learn how to guide their children and where to find help to reduce online risks.

Your front door may be locked and dead-bolted, but if your computer isn't properly secured and used safely, it offers an open window into your home.

Together we can help our children learn by taking advantage of exciting technology while reducing risks to their safety.

Roy Cooper
Attorney General





4 Background: Online Risks for Children

6 Solicitation by a Child Predator
- How It Can Happen
- The Grooming Process
- Cyberstalking
- FBI Warning Signs
- Tips for Parents

26 Unwanted Exposure to Sexual Material
- How It Can Happen
- Tips for Parents

34 Threats or Harassment Online
- How It Can Happen
- Tips for Parents

38 How to Talk to Your Child About Internet Safety
- Family Rules

42 Internet Safety: Some Closing Thoughts

44 Update: Blogs, Networking and Photo-Sharing Sites

NOTE: THIS PUBLICATION USES THE TERM "CHILD PREDATOR" AS A CONVENIENT WAY TO REFER TO AN ADULT WHO SEEKS CHILDREN. HOWEVER, EXPERTS WARN THAT THE STEREOTYPE OF A CHILD PREDATOR (FOR EXAMPLE, A SUSPICIOUS-LOOKING STRANGER WEARING A TRENCH COAT) IS INACCURATE. PARENTS SHOULD BE AWARE THAT ANY ADULT COULD BE SOMEONE WHO WOULD EXPLOIT THEIR CHILD. SEE PAGE 10.

1 in 5 youths between the ages of 10 and 17 has received unwanted sexual solicitations online [1]

1 in 4 youths has been exposed to sexually explicit pictures online without seeking or expecting them [1]

1 in 17 youths has been threatened or harassed online [1]

1 in 33 youths has received an aggressive solicitation to meet somewhere [1]

Millions of children under the age of 18 are using the Internet every day, and the number of children who are spending time online will continue to grow. This relatively new communication tool presents a variety of risks for these children.

They include:

SOLICITATIONS BY CHILD PREDATOR

Most North Carolina parents (60%) felt their children are at some risk of being contacted or preyed upon by someone they do not know while on the Internet.[2]

UNWANTED EXPOSURE TO SEXUAL MATERIAL

Most North Carolina parents (80%) expressed concern about sexually explicit materials on the Internet.[2]

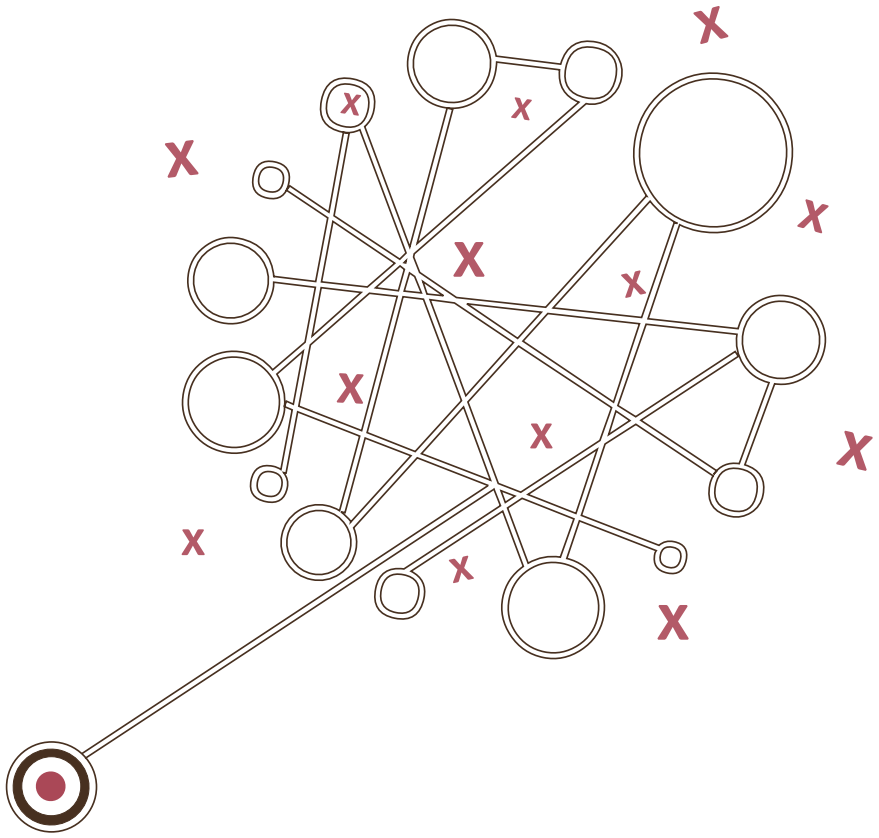
THREATS OR HARASSMENT ONLINE

Only about half of the children who were threatened or harassed reported the incident to their parents.[3]

[1] David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. Online Victimization: A Report on the Nation's Youth. Alexandria, Virginia: National Center for Missing & Exploited Children, 2000, page ix. Funding provided by Office of Juvenile Justice and Delinquency Prevention, United States Department of Justice.

[2] Children's Internet Use: An Online Survey of Concerned North Carolina Parents. North Carolina Department of Justice, 2004, page 6. Funding provided by Office of Justice Programs, United States Department of Justice.

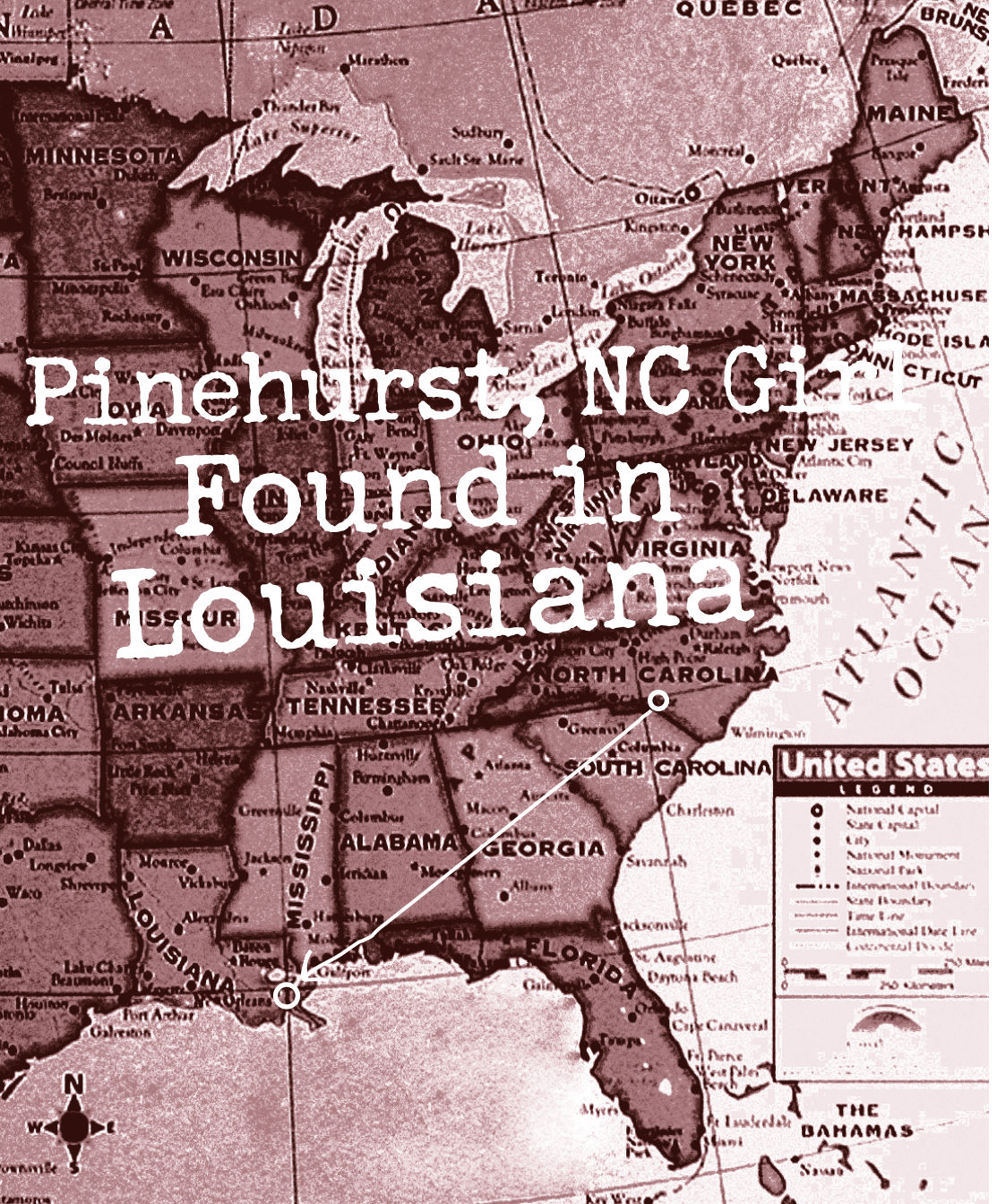
[3] David Finkelhor, Kimberly J. Mitchell, and Janis Wolak.Online Victimization: A Report on the Nation's Youth.



The Internet makes it easy for predators to locate potential victims and communicate with them. Ultimately they want to lure children into a face-to-face meeting, or get enough information to stalk the child by searching online for clues to determine a home address. That's why it is important for you to understand how predators target children.

the Internet makes it EASY for predators to locate

POTENTIAL VICTIMS



In February 2002, a 14-year-old Pinehurst, N.C. girl left home. Her parents contacted local police, who sought help from the North Carolina State Bureau of Investigation (SBI). SBI agents found a number of files on the girl's computer, including email messages. They also discovered that the girl had searched online for bus schedules and maps. Investigators were able to retrieve all of the search information and email files, which indicated that THE GIRL HAD MET A MAN ON THE INTERNET. An employee at the bus station recognized the girl's photo and told investigators that she had departed for New Orleans with a man. Using information recovered from the girl's computer, SBI agents were able to pinpoint an address in New Orleans. Agents contacted officials in Louisiana, and the girl was located and returned to her parents. Law enforcement officials in Louisiana placed the man under arrest.

Source: State Bureau of Investigation; Martha Quillin, "Missing girl is found safe in Louisiana," Raleigh News & Observer, February 15, 2002.

CHILD PREDATOR CHARACTERISTICS

While most offenders are male, law enforcement experts say that a child predator can be anyone: male or female, young or old. They often hold respectable jobs and positions in their community. People who want to harm or exploit children tend to relate more easily to children than adults, and they may also seek employment or volunteer at a children's organization.

CHILD VICTIM CHARACTERISTICS

Law enforcement officials also advise that **ANY** child can be vulnerable to a predator's enticement, including those who may be performing well at school and socializing with a "good" crowd of friends. You may believe that your child can't fall victim to a child predator. However, experts stress that such thinking can lead to a false sense of security about your child's safety.

Most children who agree to meet face-to-face with an adult do so willingly, they are not tricked or coerced

CHAT ROOMS AND NETWORKING SITES

The Internet gives users a variety of ways to communicate with each other. Some, like email and chat rooms, offer apparent anonymity. Others, like an individual's blog or personal page on a networking site, may plainly indicate the user's identity. Regardless of which method they are using to communicate, teens and preteens feel safe at a computer. But adults who are seeking children will use any means possible to observe, approach, and then groom their victims. That process frequently ends with an attempt to lure a child to a meeting outside of the home. For more information about blogs and networking sites, see the Update at the end of this resource guide. For tips and suggestions for parents, visit WWW.NCDOJ.COM

PREDATORS CAN BE EXTREMELY CONVINCING

THEY ALSO RELY ON THE INEXPERIENCE OF THEIR POTENTIAL VICTIMS, AND THEY KNOW WHAT TO SAY AND DO TO GAIN THEIR TRUST. A RECENT STUDY FOUND THAT MOST CHILDREN WHO AGREE TO MEET FACE-TO-FACE WITH AN ADULT DO SO WILLINGLY. THEY ARE NOT TRICKED OR COERCED.[4]

[4] David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. *"Internet-Initiated Sex Crimes Against Minors: Implications for Prevention Based on Findings from a National Study"* 35 Journal of Adolescent Health 11 (2004).

THE SEARCH FREQUENTLY BEGINS IN A CHAT ROOM

The search for a potential victim frequently begins in a chat room. A CHAT ROOM is a place online where people can go to "talk" with each other by typing messages. These messages are usually displayed almost instantly. Those in the chat room can view all of the conversations taking place at once on their computer screen. Chat rooms may be divided into categories. For example, an adult looking for a child victim in North Carolina may visit the "North Carolina" chat room for teenagers. For more information about chat rooms, see the inside back cover of this resource guide.

A predator pays close attention to the conversations taking place in the chat room and to the participants' screen names or user names. A SCREEN NAME is the name a participant uses to represent himself or herself online. A screen name of "jessica13country," for example, might indicate that the child is a 13-year-old female named Jessica who is interested in country music. Knowing this information, an adult who is seeking to exploit or harm a child may then assume an identity that would be likely to attract the attention of that child. If they assume the screen name of "kennychesneyguy," for instance, the girl might believe the person she is chatting with is a male fan of country musician Kenny Chesney.

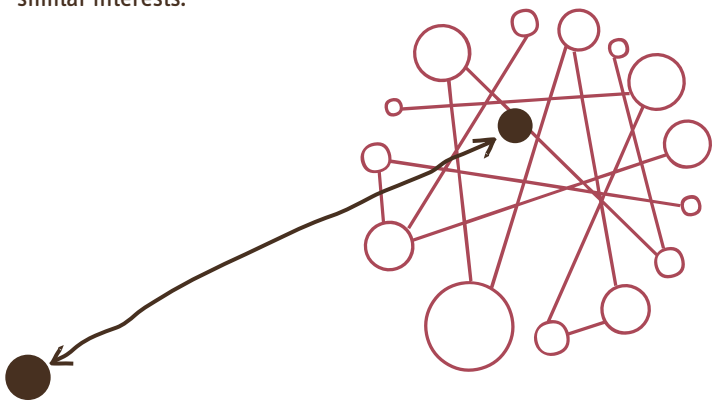
Predators can use screen names to track down a child

FINDING SIMILAR INTERESTS

Even if a predator does not gather revealing or useful information from a child's screen name, he or she can still use the screen name to determine whether the child has completed an online profile. An **ONLINE PROFILE** may contain personal information such as a child's email address, interests, and hobbies. Once a profile has been located, the person who has obtained it can easily send email or instant messages directly to the child.

Online profile pages are a central element of blogs and networking sites. For more information, see the Update at the end of this resource guide. For tips and suggestions for parents, visit www.ncdoj.com

EMAIL is a method of sending messages electronically from one computer to another. **INSTANT MESSAGING** is a service that alerts users when friends are online and allows them to communicate with each other in real time through private online chat areas. An adult who is seeking children can use the interests and hobbies located on the child's online profile to convince the child that he or she has found someone who has similar interests.



With time and research someone who is stalking your child may be able to find his way right to your door

KEEPING THE RELATIONSHIP A SECRET

After establishing a shared interest, a predator will work to build trust and convince the child that the predator is a better friend to the child than other friends or even family members. As the grooming process continues and the predator cements the relationship with the child, the predator will also ask the child to keep the relationship secret.

If youngsters seek the comfort and support of someone they've met online while keeping that relationship secret from their families, trouble often follows. Later, this secrecy may even be used as a weapon against the child. An adult who wants to exploit a child may threaten to expose the relationship to the child's parents or even threaten to harm the child or his or her family if the child tries to end the relationship.

USING THE TELEPHONE AND SETTING UP THE MEETING

At some point, the predator will usually engage in phone conservations with the child victim. The ultimate goal of the grooming process is to arrange for a face-to-face meeting with the child.

CYBERSTALKING

GATHERING PERSONAL INFORMATION

In addition to gathering personal information about a child through an online profile, a chat room discussion, or the child's screen name, a predator might also use an online discussion group. Discussion groups are like a public electronic bulletin board, where participants can read and add (or "post") comments about a specific topic. Using an email address obtained from a child's online profile, someone who is seeking to exploit or harm a child can join a group and look for items the child has posted that contain more information. For instance, if a child has posted an item for sale, they might have provided a telephone number where buyers can call for more details. From there, the predator can narrow the search.

FROM TELEPHONE AREA CODE TO HOME ADDRESS

A predator can use the telephone area code and online resources to determine the state where the child resides. They may be able to use the telephone number to determine the last name of the family and even their address. With time and research, someone who is stalking your child may be able to find his way right to your door.

Adults who are seeking to exploit children often supply their potential victims with pornography as a means of opening sexual discussions and for seduction

> do u wanna c what i look like?

The Federal Bureau of Investigation has compiled a list of warning signs that can indicate when a child might be at risk online. These warning signs can be found in the FBI's Parent's Guide to Internet Safety:

TIME SPENT ONLINE

YOUR CHILD SPENDS LARGE AMOUNTS OF TIME ONLINE, ESPECIALLY AT NIGHT. Most children who fall victim to child predators spend large amounts of time online, particularly in chat rooms. Child predators can be online at any time, but most work during the day and spend their evenings online trying to locate and lure children.

PORNOGRAPHY

YOU FIND PORNOGRAPHY ON YOUR CHILD'S COMPUTER. Pornography is often used in the sexual victimization of children. Adults who are seeking to exploit children often supply their potential victims with pornography as a means of opening sexual discussions and for seduction. Child pornography may be used in an attempt to show the child victim that sex between children and adults is "normal." Keep in mind that a child might hide pornographic material by storing it on a disk, especially if other family members use the computer.

PHONE USE

YOUR CHILD RECEIVES PHONE CALLS FROM SOMEONE YOU DON'T KNOW OR IS MAKING CALLS, SOMETIMES LONG DISTANCE, TO NUMBERS YOU DON'T RECOGNIZE.

Predators enjoy exchanging messages with children via computer. However, in most cases, they also want to talk to them on the telephone and they often engage in "phone sex" with the children. At some point, they will usually attempt to set up a face-to-face meeting for real sex.

Predators can also use these telephone calls to learn more about the children they are pursuing. If a child is hesitant to give a phone number, predators can use caller ID to determine the telephone number of the child who is calling. Some even obtain toll-free numbers so their potential victims can call without their parents finding out. Sometimes a child will be instructed to call collect. In each of these instances an adult who is seeking to exploit children can get a child's phone number, and such a predator may be able to use the telephone number to determine the child's full name and home address.

UNSOLICITED MAIL AND GIFTS

YOUR CHILD RECEIVES MAIL, GIFTS, OR PACKAGES FROM SOMEONE YOU DON'T KNOW.

As part of the grooming process, it is common for predators to send letters, photographs, and gifts to their potential victims. Some have even sent airline tickets to children, so the child can travel across the country to meet them.

When a child turns the computer monitor off or changes the screen on the monitor they are attempting to conceal something

CONCEALING COMPUTER CONTENT

YOUR CHILD HIDES WHAT THEY ARE DOING ON THE COMPUTER.

When a child turns the computer monitor off or quickly changes the screen on the monitor, they are attempting to conceal something. A child looking at pornographic images or having sexually explicit conversations does not want you to see it on the screen.

BEHAVIOR CHANGE

YOUR CHILD BECOMES WITHDRAWN FROM THE FAMILY.

Adults who are seeking to exploit children work hard to drive a wedge between a child and their family. Any problem that a child has at home can be manipulated to make that child feel isolated from their loved ones, and children under the influence of a predator may pull away from their families. Children may also become withdrawn after they have been victimized sexually.

USING DIFFERENT ONLINE ACCOUNT

YOUR CHILD IS USING ANOTHER EMAIL ACCOUNT.

Even if your child already has an email account, a child predator might set up another account so they can have more privacy when they communicate. Some online entities offer free email services, so email accounts can be created quickly and without cost. If your child is using an account other than the one you may have authorized, he or she may be communicating with someone who wants to keep the relationship secret. Keep in mind that your child could still meet and exchange messages with an adult while online at a friend's house, the library, or at school.

FOR 24 HOUR CHILD ABUSE CRISIS COUNSELING CALL 1-800-4-A-CHILD (1-800-422-4453).

TO LOCATE ORGANIZATIONS AND RESOURCES IN YOUR AREA, GO TO WWW.NCDOJ.COM. FROM THE "JUMP TO" MENU, SELECT "INTERNET SAFETY." CLICK ON "PARENTS" AND THEN "ADDITIONAL RESOURCES."

IF YOU HAVE QUESTIONS ABOUT CHILD VICTIMIZATION, YOU MAY WANT TO CONTACT YOUR PEDIATRICIAN.

Source: Federal Bureau of Investigation

MINIMIZE RISKS

Parents can minimize the risk of a child meeting an online predator by taking some SIMPLE steps.

CONTROL ACCESS

Adults who are seeking to exploit children spend countless hours in chat rooms and networking sites. Many experts believe that these sites are not safe for children, particularly young children. If you decide to allow your child to enter chat rooms or join a networking site, make sure your decision is based on their age and maturity. Children who are allowed into chat rooms and networking sites need additional supervision. For more information about networking sites, see the Update at the end of this resource guide. For tips and suggestions for parents, visit **WWW.NCDOJ.COM**.

CONTROL INSTANT MESSAGING

Like email and chat rooms, instant messaging (or "IMing") can be used to communicate secretly. Children often use abbreviations and code (such as "POS" which means "parent over shoulder") to change the course of the conversation when parents are watching and to keep parents from understanding online conversations.

KEEP SCREEN NAMES ANONYMOUS

Predators can use screen names to track down a child. Parents should make sure that their child's screen name does not include personal information such as name, age, home address or school name.

AVOID ALL ONLINE PROFILES

Many websites offer users the opportunity to set up an online profile where they can provide information about themselves. This is a central element of networking sites. However, this information can be accessed and used by predators. One way to protect your child's privacy is for him or her to avoid these online profiles. For more information about networking sites, see the Update at the end of this resource guide.

TAKE CARE WITH PHOTOGRAPHS AND CAMERAS

Computers make it easy to send and share photographs, but it should be done carefully. Children should not send photos to anyone, including other children, without parental approval. For important information about photo sharing sites and the misuse of digital images, see the Update at the end of this resource guide.

READ EMAIL, BLOGS AND NETWORKING SITES

Experts recommend that parents monitor their child's online activities regularly. To some parents this may seem like an invasion of privacy. But email, chat room conversations, instant messages, and entries on blogs and networking sites are not like entries in a diary. They are an open window to your child's life, carrying information to and from your home. Parents should share an email account with their child or maintain access to their child's email account and check it frequently. Children who are allowed to chat or use instant messaging, blogs or networking sites also need extra supervision.

PLACE COMPUTER IN COMMON AREA

You should place your computer in a central room of the house, in order to monitor what your child is doing online. The computer screen should face out, into the room, so it is easy for you to see. Develop a list of family rules for using the Internet (see sample Family Rules) and post it next to the computer.

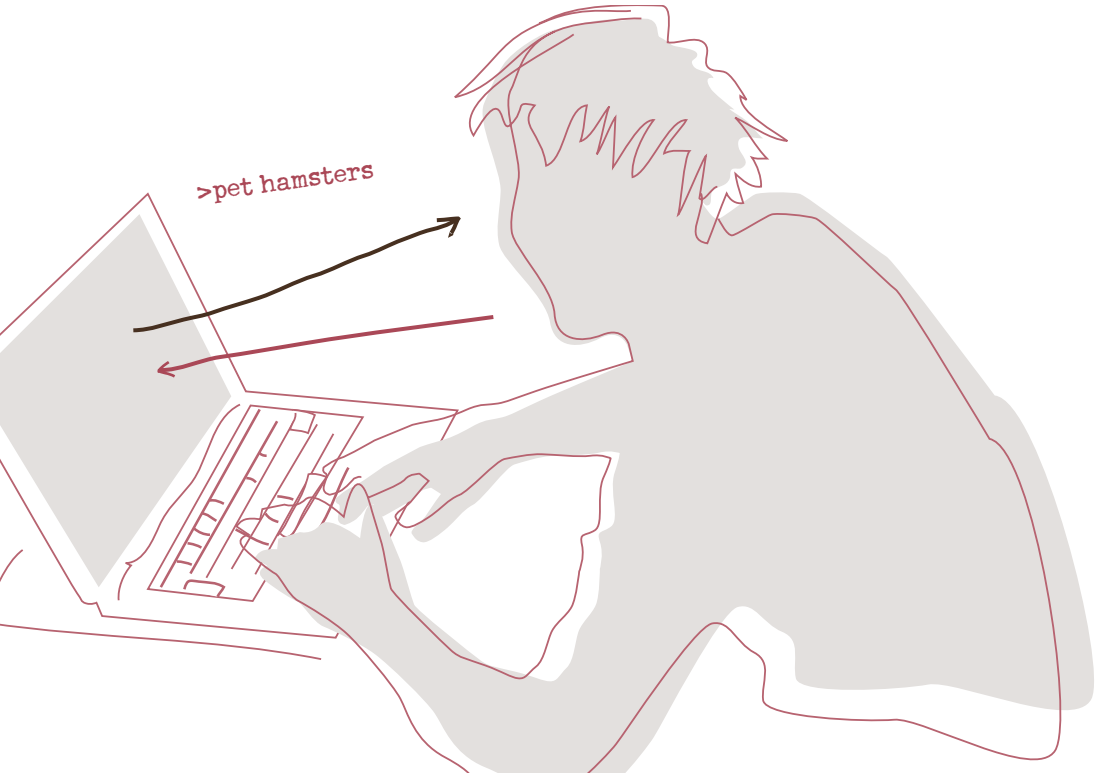
keep an eye on what your children are doing online

REMIND CHILDREN THAT COMPUTER USE IS NOT CONFIDENTIAL

Children want to be treated as adults, and they feel entitled to privacy. But with a computer, you can go too far in trying to respect your child's privacy. Children should not have the expectation that everything they do on a computer will be considered personal and confidential.

Sources: North Carolina State Bureau of Investigation and the North Carolina Internet Crimes Against Children Task Force

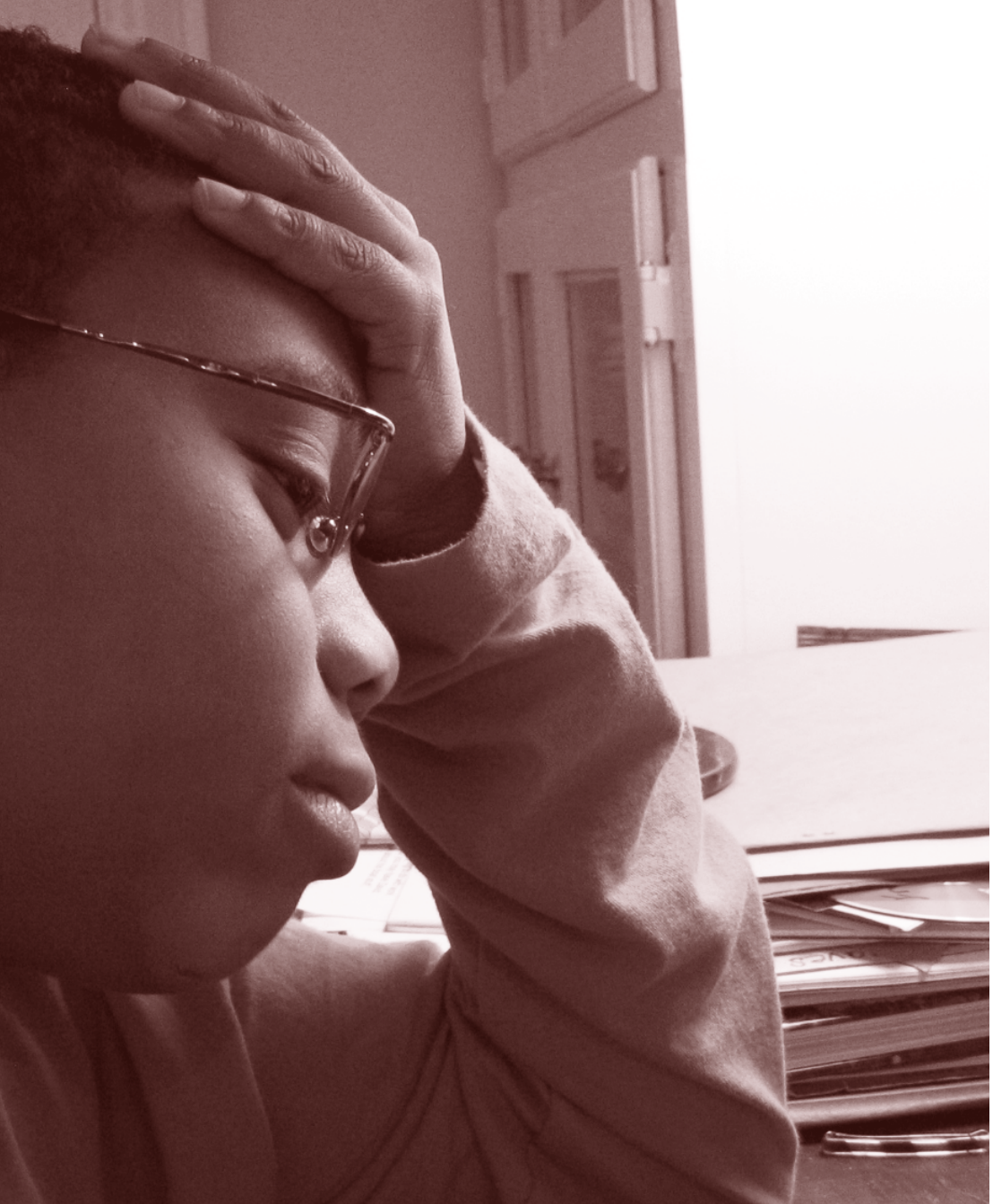
searching the words "toy" or "pet" can bring up sexual material



While some children seek out sexual material online, a study by the National Center for Missing & Exploited Children found that 25 percent of youth had experienced unwanted exposure to sexual pictures on the Internet. In fact, children might accidentally come across a website they weren't looking for, either by misspelling a word, typing the wrong domain name or by using search terms. Even searching the words "toy" or "pet" can bring up sexual material. Unsolicited email (commonly known as "spam") can also expose children to sexually oriented material.

To keep your child from accessing or being exposed to websites that contain inappropriate sexual material, it is important to have an understanding of how the Internet works. Let's start at the source of the Internet, the data that streams in and out of your home. Your computer connects to the online world through your Internet Service Provider (ISP).

Your ISP may be a company like America Online (AOL), Microsoft Network (MSN) or EarthLink. Many telephone companies and cable television companies are also ISPs. Regardless of which company connects your computer to the Internet, your ISP can play an important role in making your family safer online.



CONTACT YOUR ISP FOR HELP

The company that provides your Internet service can help you control what your child can and cannot access on the Internet. However, according to some ISPs, parents rarely take full advantage of these services. **Parents are strongly encouraged to contact their ISP to learn about the parental control features it offers.** Increasingly, ISPs are offering controls for free or at a small charge. In either case, the company has a technical support staff to help you. If you want to learn more about your company's features or how to set up the parental controls yourself, go to the company's website. For more information on how to find out about your ISP's parental control features, visit **WWW.NCDOJ.COM**.

USE YOUR COMPUTER'S PARENTAL CONTROLS

In addition to the parental controls available through the ISP, you can use the computer itself to help make the Internet a safer place for your children. For instance, you can set up the computer so a child only has access to certain approved websites.

This process may seem daunting, but the computer can assist you in setting up parental controls. Most computers contain some form of a "Help" menu. You should access it and type "Parental Control." The computer will present a list of topic information based on those words. Clicking on a topic will bring more information. One of the first things your computer will do is instruct you to set up individual logins for each family member.

Parents can also check a record of the websites that have been visited. These are often found under "History." The websites offer clues about your child's online activities.

For instance, if your child has a secret email account, the Internet History may indicate visits to the site that hosts the email account.

You can set up the computer's parental controls to prevent the Internet History from being altered or deleted by your child.

ASSISTANCE IS AVAILABLE

If you aren't able to set up parental controls on your computer, here are some other options:

- **CONTACT TECHNICAL SUPPORT**
  Call the computer or software company's technical support number, or send the company an email. Software means the programs you use to access the Internet like Microsoft Internet Explorer or Netscape.
- **ARRANGE FOR A HOUSE CALL**
  Contact a local computer technical support company that makes house calls. For a fee, a technician can come directly to your home, set up the parental controls for you, and show you how to use them.
- **CONTACT FAMILY AND FRIENDS**
  Many of us have a family member or a friend who is more computer-savvy than we are. If you are having difficulty setting up parental controls, ask that person to assist. They may be willing to help.

CONSIDER INSTALLING FILTERING AND BLOCKING SOFTWARE

You may also want to acquire additional parental control software that limits what your child can access. Filtering devices can add another level of security, although many people find that the controls available on their computer and through their ISP are sufficient.

1-800-THE-LOST

REPORT SUSPICIOUS ACTIVITY

If your child or anyone in the household has received child pornography, contact local law enforcement. You should also contact authorities if your child has received obscene material from someone who knows that your child is under the age of 16. You may also call

1-800-THE-LOST (1-800-843-5678)
or visit WWW.CYBERTIPLINE.COM.

Threats and harassment are no longer limited to the playgrounds or daytime hours. The Internet now makes it possible for bullies to torment their victims in their home and at any time of the day. These "cyberbullies" may use chat rooms, email, instant messaging, and web-sites to embarrass a child. Tech-nology allows them to share gossip, spread lies or distribute embar-rassing pictures to a wide audience while maintaining some anonymity. Not surprisingly, one in every 17 kids reported being threatened or harassed while using the Internet.[5]

[5] David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. Online Victimization: A Report on the Nation's Youth.

If someone threatens your child with violence, immediately contact law enforcement officials.

SAVE THE ORIGINAL MESSAGE

Don't delete or erase threatening emails or other communications from your mailbox or voicemail. If you are asked to share a threatening email message with law enforcement, forward the original message. A printed copy of the email or an excerpt from it will not be as useful to law enforcement as the original email message that you received.

If your child is being threatened or harassed online, you may want to contact one or more of the following:

SCHOOL RESOURCE OFFICER

Your child's school may have a School Resource Officer (SRO), a sworn law officer assigned to their school. If so, let the SRO know about the harassment or threats. If your school does not have an SRO, contact local law enforcement.

INTERNET SERVICE PROVIDER

Your email account settings or instant messaging software may allow you to block further messages from the sender. You can report the harassment or threats to your ISP and the harasser's ISP if you know which ISP the harasser uses. You can ask that the harasser's account be suspended or blocked.

CYBERTIPLINE

If your child receives invitations for sexual acts or unsolicited obscene material over the Internet, you can report it by calling 1-800-THE-LOST (1-800-843-5678) or by visiting WWW.CYBERTIPLINE.COM.

As parents,
we can't afford to let our
children's knowledge
OUTSTRIP OUR OWN!

IN A CALM MANNER, TELL YOUR CHILD WHAT IS DANGEROUS ABOUT THE INTERNET

THIS CAN INCLUDE:

- Legal or financial harm to the family, if you "click" without getting permission
- Exposure to harmful material (violence or sexually explicit scenes)
- People online who may start off friendly but then change

Even the youngest child can understand the old adage "don't talk to strangers." Teach children from an early age that this includes people who try to talk to them online

TALK TO YOUR CHILDREN ABOUT POTENTIAL DANGERS

ENCOURAGE THEM TO TELL YOU WHEN:

- Someone they don't know attempts to engage them in an online chat
- An inappropriate site comes up on the screen
- Someone harasses or threatens them online

Ask your child to tell you when anything questionable happens to them online. Make it clear that they will not lose Internet privileges or be punished if they tell you

TEACH YOUR CHILDREN ABOUT THE DIFFERENCES BETWEEN "PRETEND" AND REALITY ON THE INTERNET

- Many children like to pretend to be someone else while online
- They feel they are anonymous and can take risks
- However, other people also like to pretend to be someone else while online
- But they do it for totally different reasons. Sometimes they do it to hurt people

Children need to understand that real world rules and values apply on the Internet as they do in real life

DON'T JUST TELL YOUR CHILDREN WHAT THEY CAN'T DO

- Make a point to sit with your children and see the sites they like to visit
- Explain why you think a site is inappropriate

MAKE IT CLEAR TO YOUR CHILDREN THAT YOU ARE IN CHARGE

- Children may not realize it, but they need supervision
- Remind them that you have more experience dealing with the world

Your children must understand that just as you decide which movies they are allowed to see, you will supervise their online activities.

A RECENT STUDY FOUND THAT MOST CHILDREN DID NOT INFORM THEIR PARENTS WHEN THEY FACED A DIFFICULT SITUATION ONLINE, SUCH AS BEING CONTACTED BY SOMEONE THEY DON'T KNOW.

THE MAIN REASONS FOR THEIR HESITATION WERE EMBARRASSMENT AND FEAR OF LOSING ACCESS TO THE INTERNET.

Sources: National Center for Missing & Exploited Children and the North Carolina Internet Crimes Against Children Task Force

CREATING FAMILY RULES FOR INTERNET USE

SOME OF THE DECISIONS TO CONSIDER IN CREATING FAMILY RULES WOULD INCLUDE:

- Do you want your children to ask you before they access the Internet?
- Do you want to limit the time your children access the Internet? If so, how much time per week or day?
- Do you want to specify when your children may access the Internet? If so, which hours?
- Do you want to permit your children to use email? If so, do you want to share an email account with them or have access to their account?
- Do you want to permit your children to use instant messaging? If so, do you want to approve their "buddies" list and require them to provide you with an updated copy of that list?
- Do you want to permit your children to enter chat rooms and networking sites? If so, do you want to limit them to certain ones that you have approved?

When possible, have your family computer rules in place before your children begin using the computer. Children will find it easier to accept and obey rules that have already been established.

SAMPLE FAMILY RULES FOR INTERNET USE

USING THE COMPUTER IS A PRIVILEGE. IN ORDER TO ENJOY THIS PRIVILEGE AND USE THE COMPUTER, WE AGREE TO FOLLOW THESE RULES:

1) Computer use is not confidential, and we do not hide what we are doing on the computer.
2) In our family, we get permission to access the Internet, and we use our personal login.
3) We visit websites that are appropriate for our age, and we do not visit websites or access information that are "off limits" for us.
4) We don't send photos or give out personal information without permission, and we will tell our parents about any online messages we receive that make us uncomfortable.
5) We share an email account with our parents. We will not open or use any other email accounts.
6) We do not enter chat rooms or networking sites.
7) We can go online between the hours of _____ and _____ .
8) Time on the computer is limited to: _____ Hour(s) per day.
9) Time on the Internet is limited to: _____ Hour(s) per day.
10) Instant messaging is only allowed with people that we already know. We will provide our parents with a current list of our "buddies."
11) We do not respond to messages from people we do not know.
12) These rules apply to our home computer and all other computers we use.

_____ name _____ date

For a printable version of these rules, go to WWW.NCDOJ.COM

SOME CLOSING THOUGHTS TO KEEP IN MIND TO HELP YOU MAKE THE INTERNET A SAFER PLACE FOR YOUR FAMILY:

YOU DON'T HAVE TO BECOME A COMPUTER EXPERT

Although young people are learning about computers at an early age, parents can exercise control over their children's use of computers and the Internet without having to become computer experts. As parents, we can't afford to let our children's knowledge outstrip our own. We owe it to them to supervise and control their use of this powerful technology.

BE ON THE LOOKOUT FOR ADVANCES IN TECHNOLOGY

For instance, your ISP may announce that it has developed new parental control tools. If so, you might have to download or activate them. These upgrades may help you better control what your child can access on the Internet. You should review your existing parental controls periodically. Make sure they are still appropriate and update them.

SPEND TIME WITH YOUR KIDS, OFFLINE AND ONLINE

Remember, the computer is a great communication tool but you are an even better one. The best way to make sure your children aren't getting into trouble on the Internet or anywhere else in their lives is to stay engaged with them. Get them to show you what they do on the computer, and the websites they visit. Ask them about anyone they've met online, and familiarize yourself with those people.

IT ISN'T SNOOPING, IT'S CARING

MONITOR YOUR KIDS WHILE YOU TEACH THEM INTERNET SAFETY

Unfortunately, there are real dangers lurking on the Internet. Some parents say they don't feel comfortable checking up on their child's computer activities. It is understandable that a parent would want to honor their children's privacy. However, experts say that should not come at the expense of knowing what your child is doing online. It isn't snooping, it's caring.

The Attorney General's Office can provide Internet safety programs for North Carolina's children, parents and educators. We also can help with your questions about Internet safety. To request a presentation or ask a question, go to WWW.NCDOJ.COM. From the "Jump To" menu, select "Internet Safety." Then click on "What is ICAC?" and scroll to the bottom of the page for contact information.

UPDATE: INTRODUCTION

Internet trends can develop quickly.

Since the first publication of this resource guide, the use of networking sites, photo-sharing sites and "blogs" has exploded, especially among children. But as new hardware, software and related technologies come online and gain popularity among young people, new dangers follow.

The Internet is still a wonderful communication tool. But child safety experts continue to warn parents that any part of the Internet that allows people to exchange messages and information can be used by adults who are seeking to exploit children.

This **UPDATE** is designed to supplement the existing information in this resource guide. Parents should read the entire guide. The material on pages 44-48 provides information about networking sites and other recent online developments. For tips on how to deal with these new developments and the very latest Internet safety information, visit **WWW.NCDOJ.COM**.

Any part of the Internet that allows people to exchange messages can be used by adults who are seeking to exploit children

BLOGS

The term "**BLOG**" is a shortened form of "web log." A blog might detail the thoughts and daily activities of its creator, or be devoted to commentary about a sports team or performer. The creator of a blog writes comments for visitors to read and visitors can respond by "posting" a reply to those comments. Visitors can read each other's comments and begin communicating directly with each other.

Dangers associated with blogs are similar to those associated with chat rooms. Adults who are seeking to exploit children can visit youth-oriented blogs and strike up online conversations. Another similarity: young blog creators and visitors may divulge too much personal information about themselves. This information can draw the attention of a child predator, and it may also provide a way for a predator to determine the location of a potential victim.

Blog creators and visitors may divulge too much personal information about themselves

THINK BEFORE YOU POST

In addition to the dangers posed by online predators, comments posted on a blog or a networking site can come back to haunt the young person who writes them. Words that may have been intended for a small audience sometimes find their way to a larger one, especially if they are controversial. Some parents have been shocked to see what their children have written online. Students who have posted threatening words against their school or classmates have attracted the attention of school administrators and even law enforcement. Many university administrators or potential employers also search the web for information posted by a prospective enrollee or employee.

Networking sites, photo-sharing sites, chat rooms, blogs and even online gaming sites are places on the Internet where a child predator can meet and begin communicating with a young person.

MySpace, Friendster, Facebook, and Xanga are examples of **NETWORKING SITES.** These are sometimes referred to as "Social Networking sites" because they allow members to communicate with each other. On most networking sites, communication is unrestricted and unsupervised. The sites encourage users to reveal personal information and interests, which is then posted online in a member profile or personal page. Members can also post photographs.

PHOTO-SHARING SITES, like Album, Flickr, and Photolog, also allow members to post photos for others to see. Some photos on these sites are available for unrestricted viewing, while others may be in password-protected areas. Like networking sites, these sites also allow commentary and messaging among users.

FOR TIPS ON HOW TO DEAL WITH THESE NEW DEVELOPMENTS AND THE VERY LATEST INTERNET SAFETY INFORMATION, VISIT WWW.NCDOJ.COM.

Young people don't always think about the long-term repercussions of their actions. They may not be able to foresee the potentially embarrassing and dangerous consequences of misusing this technology.

Networking sites and photo-sharing sites are also related to another area of growing concern regarding children and the Internet. This problem centers on the inappropriate use of digital cameras and web cameras (or "webcams"). Just as parents and guardians monitor and control their children's use of the Internet itself, they need to supervise and oversee the use of these photographic tools.

Before the advent of digital cameras, concerns about privacy kept most camera users from taking or posing for revealing photos. **DIGITAL CAMERAS**, especially easy-to-use versions marketed to children, have made it simple to take pictures that no one else sees. Computers have made it easy to post or email these photographs. Some young people are experimenting with this technology while exploring their sexuality by taking explicit or revealing pictures of themselves or others.

Some young people are also using computer-based cameras, known as webcams, to transmit sexually explicit images of themselves. **WEBCAMS**, which are inexpensive and often no bigger than a golf ball, are usually placed on top of a computer monitor. When connected to a computer, these cameras send video images that can be viewed instantaneously by one or more computer users. Adults who seek to exploit children sometimes mail webcams to children they have met on the Internet to facilitate online sexual encounters.

CAMERA PHONES CAN ALSO BE MISUSED.

Because camera phones are always at hand, they make it easy to take photos on the go. They also make it easy to take inappropriate photos. In some cases the subject may not have given permission for the photo to be taken, or even know they've been photographed. And camera photos can be uploaded to a computer just as easily as photos from a standard digital camera.

Unfortunately, suggestive photos that were intended for only one person may eventually be shared with a larger audience. A boyfriend or girlfriend can become an "ex," and secret passwords don't always stay secret.

Computer crime investigators report that when students find an inappropriate photograph of a classmate, the photograph (or the password that allows access to it) often circulates throughout the school. The image may be seen by many students before it comes to the attention of school officials, causing great embarrassment to the student who is pictured. In addition, law enforcement investigators must visit the student's home to determine whether an adult had any involvement in the production or distribution of the photo.

Once the photograph has made its way to the Internet, it is nearly impossible to remove. It can be altered or misused by those who have access to it, and it remains in circulation forever.

ADDITIONAL RESOURCES

AGE-APPROPRIATE SEARCH ENGINES

These age-appropriate search engines greatly reduce the possibility of exposure to inappropriate material:

- **LEARN NC (learnnc.org/bestweb)** - Learn NC's "Best of the Web" collection provides a searchable, annotated catalog of more than 3,000 educational websites.
- **KIDSCLICK** (kidsclick.org) - Created by librarians to guide young users.
- **ASK FOR KIDS** (askforkids.com) - A site focused on learning.

WHAT'S IN A DOMAIN NAME?

A domain name that ends in **.gov** is a government website. Domain names that end in **.edu** are affiliated with an educational facility. These are unlikely to contain inappropriate material. While the majority of domain names that end in **.com, .org, or .net** are suitable for children, many are not.

CHAT ROOM AND INSTANT MESSAGE ABBREVIATIONS

Young people have developed many shortcuts to save time and to keep adults in the dark:

DIKU → Do I know You?
A/S/L → Age/Sex/Location?
LMIRL → Lets meet in real life
POS → Parent over shoulder

For more examples of chat abbreviations visit www.ncdoj.com. Under Internet Safety, see "Additional Resources for Parents," then locate the listing for the National Center for Missing & Exploited Children.

NC STATE UNIVERSITY

DESIGNED BY CAROLINE OKUN
ILLUSTRATIONS BY CAROLIN HARRIS

Do you know what your child is doing online?

Things are changing fast in the online world. For the very latest Internet safety information, visit www.ncdoj.com

ncdoj.com